REMARKS

Claims 1 – 124 are pending in the Application. Claims 1, 69, 109, and 110 are currently amended. New Claims 125 and 126 are currently added.

Claim Objections

The Examiner suggested that "transport data monitor being operable to monitor" in claim 13 should read "transport data extractor being operable to monitor".

Applicant maintains that claim 13 should recite "transport data monitor being operable to monitor", as originally defined, in accordance with the description provided by the disclosure on page 8, in lines 21-23: "Preferably, the network is a packet-switched network, the data being transported comprises passing packets and the transport data monitor is operable to monitor header content of the passing packets".

Claim Rejections – 35 USC 102 & 103

In this section of the official action, Claims 1-4, 11, 51, 56-65, 69, 70, 109, 110, 111, and 112 were rejected under 35 USC 102(e) as being anticipated by Kephart US Patent No. 6,732,149.

The Examiner further rejected claims 69, 70, 73, 86, 87, 91-99 under 35 USC 103(a) as being unpatentable over Kephart US Patent No. 6,732,149 in view of Olnowich US Patent No. 6,389,476.

Favorable reconsideration of this rejection in view of the above amendments and the following explanations is respectfully requested.

The present application describes a system for network content monitoring and control. The system described by the present application relates to the monitoring of digital content, for enforcing copyright, secrecy, and confidentiality with respect to the transported digital content. The present application defines in the field of invention section: "The present invention relates to monitoring transport of digital content, particularly but not exclusively for the enforcement of digital copyright, secrecy, and confidentiality".

The present invention aims at controlling the movement of content of known documents, *internally generated in the organization's network in advance of the*

movement of the content, thereby providing a proactive protection for the content, before an event of unauthorized or undesirable dissemination has occurred.

With the present invention, transported digital content is examined. If the examined digital content is identified as bearing content of a known document *internally generated by the organization*, where the known content is confidential, secret, protected by copyright, etc, the movement of the digital content identified as bearing content of the *internally generated* document may be limited according to a predefined policy with respect to the specific document.

Kephart US Patent No. 6,732,149 teaches a system and a method for protection against SPAM, as described in the field of invention section: "the present invention relates to a system and method for automatically detecting and handling unsolicited and undesired electronic mail such as Unsolicited Commercial E-mail (UCE), also referred to as "spam".

Kephart examines electronic mail for determining if the mail bears patterns of SPAM, and blocks such mail. If a message is found as undesirable, the system applies a policy with respect to similar messages, but the whole process is triggered by "determining that transmission or receipt of at least one specific electronic message is undesirable", that is, in a **reactive manner**. The present invention deals with a conceptually different **proactive protection**, where the content is first designated for protection, before an event of "undesirable transmission" occurred.

Kephart does not disclose or even hint at a method or at an apparatus where a transported message is examined for determining if the message contains content of a known document, *generated by the organization* in advance of the examination, where the content may be confidential, protected by copyright, etc, as taught by the present invention.

Olnowich US Patent No. 6,389,476 relates, as described in the field of invention section, pertains to digital parallel processing systems wherein a plurality of nodes is communicated via messages sent over an interconnection network. More particularly, the invention relates to a network adapter design for facilitating introduction of faster speed transmission products into a network including slower products.

Claim 1, as currently amended, defines a system for network content monitoring, comprising: a transport data monitor, connectable to a point in a network, for monitoring data being transported past the point, a description extractor, associated with the transport data monitor, for extracting descriptions of the data being transported, a database of at least one preobtained description of known content whose movements it is desired to monitor, *the content being internally generated in the network in advance of the extracting*, the preobtained description being obtained in advance of the extracting descriptions, and a comparator, configured to determine whether the extracted description corresponds to any of the at least one preobtained descriptions, and to decide whether the data being transported comprises any of the content whose movements it is desired to monitor according to the determining.

As described hereinabove and defined by claim 1, the present invention teaches a system which includes a transport data monitor, connectable to a point in a network, for monitoring data being transported past the point, a description extractor, associated with the transport data monitor, for extracting descriptions of the data being transported, a database of at least one preobtained description of known content whose movements it is desired to monitor, *the content being internally generated in the network in advance of the extracting*.

For example, the present application describes controlling the photocopying of documents prepossessed by an organization, on page 49, in line 13: "Reference is now made to Fig. 10, wherein there is illustrated a further embodiment of the system described in Fig. 9, specifically for preventing copying of classified documents using a photocopy machine. In this embodiment, a central control of a monitoring system 1010 is connected to a controller 10951 of copy machine 1095. Many modern copy machines contain a scanner that transforms the copied document into a digital image. The textual content of the document may be extracted from the digital image using a standard Optical Character Recognition (OCR) technique. After extraction, the textual content or derivatives thereof can be analyzed using a signature analyzer 10101 in order to determine whether the content comprises an unauthorized document. The output of the analysis is then used by a policy manager 10102 in order to determine

whether to take action and if so, what action: e.g., not allowing photocopying of the document, auditing, sending a message to the offender, etc".

The present application further describes on page 32, line 8: "The signatures of each packet are compared with the signatures in the database, and each match with any of the pre-stored signatures belonging to a particular content item that is represented in the database increases the likelihood that the data belongs to the matched content".

Kephart examines electronic mail for determining if the mail bears patterns of SPAM, and blocks such mail. However, Kephart does not disclose or even hint at the idea of a system which includes a comparator, configured to determine whether the extracted description corresponds to any of the at least one pre-obtained descriptions, and to decide whether the data being transported comprises content *internally generated in the network in advance*, whose movements it is desired to monitor, as taught by the present invention and defined by claim 1.

Olnowich US Patent No. 6,389,476 relates, as described in the field of invention section, pertains to a network adapter design for facilitating introduction of faster speed transmission products into a network including slower products.

However, Onlnowich also falls short of describing or even hinting at the idea of a system which includes a comparator, configured to determine whether the extracted description corresponds to any of the at least one pre-obtained descriptions, and to decide whether the data being transported comprises *content internally generated in the network in advance*, whose movements it is desired to monitor, as taught by the present invention and defined by claim 1.

It is thus respectfully believed that claim 1 is both novel and inventive over the prior art, and maintained that claim 1 is allowable.

Claim 69, as amended, defines a system for network content control, comprising:

a transport data monitor, connectable to a point in a network, for monitoring data being transported past the point, a signature extractor, associated with the transport data monitor, for extracting a derivation of payload of the monitored data, the derivation being indicative of content of the data, a database of preobtained signatures of known content whose movements it is desired to monitor, *the content being internally generated in the network in advance of the extracting*, the preobtained signatures being obtained in advance of the extracting the derivation of the payload, a

comparator for comparing the derivation with the preobtained signatures, and to determine whether the monitored data comprises any of the content whose movements it is desired to control, a decision-making unit for producing an enforcement decision, using the output of the comparator, and a bandwidth management unit connected to the decision-making unit for managing network bandwidth assignment in accordance with output decisions of the policy determinator, thereby to control content distribution over the network.

As described hereinabove, neither Kephart nor Olnowitch describe or even hint at the idea of a system which includes a comparator for comparing a derivation of paylaod with the preobtained signatures of known content whose movements it is desired to monitor, *the content being internally generated in the network in advance*, as taught by the present invention, and defined by claim 69.

It is thus respectfully believed that claim 69 is both novel and inventive over the prior art, and maintained that claim 69 is allowable, as taught by the present invention and defined by claim 69.

Claim 109, as amended, defines a method of monitoring for distribution of known sensitive content over a network, the method comprising: obtaining extracts of data from at least one monitoring point on the network, obtaining a signature indicative of content of the extracted data, comparing the signature with at least one of a set of signatures indicative of the sensitive content, *the sensitive content being internally generated in the network in advance of the obtaining extracts*, the set of signatures being stored in advance of the obtaining extracts of data, determining if the extracted data comprises any of the sensitive content according to the comparing, and using an output of the determining as an indication of the presence or absence of the sensitive content.

As described hereinabove, neither Kephart nor Olnowitch describe or even hint at the idea of a method which includes obtaining extracts of data from at least one monitoring point on the network, obtaining a signature indicative of content of the extracted data, and comparing the signature with at least one of a set of signatures indicative of the sensitive content, *the sensitive content being internally generated in the network in advance of the obtaining extracts*, as taught by the present invention and defined by claim 109.

It is thus respectfully believed that claim 109 is both novel and inventive over the prior art, and maintained that claim 109 is allowable, as taught by the present invention and defined by claim 109.

Claim 110 as amended defines a method of controlling the distribution of known sensitive content over a network, the method comprising: obtaining extracts of data from at least one monitoring point on the network, obtaining a signature indicative of content of the extracted data, comparing the signature with at least one of a set of signatures indicative of the presence of the sensitive content, the set being stored in advance of the obtaining extracts of data, the sensitive content being *internally generated in the network in advance of the obtaining extracts*, determining if the extracted data comprises any of the sensitive content according to the comparing, using an output of the determining in selecting an enforcement decision, and using the enforcement decision in bandwidth management of the network.

As described hereinabove, neither Kephart nor Olnowitch describe or even hint at the idea of a method which includes obtaining extracts of data from at least one monitoring point on the network, obtaining a signature indicative of content of the extracted data, and comparing the signature with at least one of a set of signatures indicative of the presence of the sensitive content, the set being stored in advance of the obtaining extracts of data, the sensitive content being *internally generated in the network in advance of the obtaining extracts*, as taught by the present invention and defined by claim 110.

It is thus respectfully believed that claim 110 is both novel and inventive over the prior art, and maintained that claim 110 is allowable, as taught by the present invention and defined by claim 110.

All dependent claims are believed to be allowable as being dependent upon an allowable main claim.

All of the matters raised by the Examiner have been dealt with and are believed to have been overcome.

In view of the foregoing, it is respectfully submitted that all the claims now pending in the application are allowable over the cited reference. An early Notice of Allowance is therefore respectfully requested.

Respectfully submitted,

Martin D. Moynihan

Martin Moynihan
Registration No. 40,338

Date: February 12, 2007

Encl.:
Petition for Extension of Time (3 Months)
Additional Claim Fee